# CyFlare End Customer Solution Terms

Effective January 1, 2025

The following solution-specific scope and terms ("Solution Terms") apply to Services purchased by the Customer ("Customer" or "you") in a signed agreement, quote or SOW. These Solution Terms are issued pursuant to the Master Service Agreement or Reseller Agreement (collectively, "Agreement") between the Customer and CyFlare Security Inc. ("CyFlare") and are subject to the terms and conditions specified below. Any term not otherwise defined herein shall have the meaning specified in the Agreement.

## General Assumptions

CyFlare's pricing, schedule, and scope of services are based on these assumptions:

- CyFlare will assign a **Customer Success Manager ("CSM")** who will be your focal point for the engagement.
- You [Customer] will identify a **liaison** who will be CyFlare's focal point of contact (e.g., scheduling, documentation collection, status reporting, and issue resolution)
- You [Customer] will share existing, relevant documentation with CyFlare (preferably in electronic formats)
- You [Customer] will not share sensitive or regulated data (e.g., PHI, PII, CUI, or CHD) with CyFlare unless mutually agreed upon and to the extent it is necessary for the services CyFlare provides. If you expect CyFlare to encounter regulated data while working with you (e.g., during pen tests), you will inform CyFlare in advance. CyFlare will protect the non-public information you share with it.
- You [Customer] will provide remote access to networks, systems, and documentation to CyFlare to perform its services.

## Change Management

We will follow this process if either party needs to make a change to CyFlare's Services:

- CyFlare will create a written Change Request (CR), including a change description, rationale, and impact.
- CyFlare will review the CR with your liaison. We may mutually agree to investigate the CR further to determine the impact on the Service price and schedule.
- After further investigation, CyFlare will update the CR documentation.
- We may mutually agree to reject or execute the CR. However, both parties must sign the CR for it to be considered executed.

# General Service Deliverables

CyFlare shall provide the following:

1. Supporting documentation outlining all required items related to services to be deployed

2. If applicable, provide access to the source XDR, VSS, Email and EDR management platforms
3. Access to CyFlare ONE
4. 24/7/365 monitoring of security alarms leveraging default and curated detections and playbooks for in-scope services
5. 24/7/365 support for all security incidents from CyFlare security analyst based on an incident response plan (to the extent the purchased platforms can provide)
6. Full security incident report in the event of a confirmed compromise within the environment (to the extent the purchased platforms can provide)
7. Monitoring the in-scope technical appliance(s) to ensure platforms are functional.
8. Monitor, investigate, and provide tickets to Customer based on the Service Level Agreement ("SLA") level subscribed to by Customer. CyFlare SLAs can be found at https://www.cyflare.com/legal
9. For applicable service offerings, fulfill up to 5 change requests per month per Customer. Change requests include:
    a. ATH Rule creation/modifications
    b. Rule filters
    c. Reporting requests
    d. Configuration changes
    e. Playbook modifications
10. Monthly or quarterly security briefing call to review the service delivery outcomes

## CyFlare Onboarding Responsibilities

CyFlare shall provide the following:

1) Provide a designated Deployment Engineer (DE) to support technical tasks associated with customer onboarding
2) Provide a named Project Manager to track logistical tasks and ensure strict delivery timelines
3) Provide access to CyFlare's Project Plan to track onboarding tasks and status
4) Schedule regular deployment sessions for project tasks to be completed
5) Operationalize and train the customer on Incident Response plan settings to determine contact procedures for related service escalations
6) Deploy the in-scope technical solutions defined by quote and/or SOW
7) Provide applicable service-related endpoint agent(s) and token(s) to Customer for deployment and/or configuration tasks
8) Provide customers with completed project plan upon onboarding task completion

## Customer Responsibilities

Customer shall provide the following:

1) The Customer will participate in scheduled onboarding calls with the provided Project Manager and Deployment Engineer (DE)
2) The Customer will work with the onboarding team to populate the customer knowledgebase document that adds context to the Customer environment and integrates with service delivery teams
3) The Customer will provide IP/Subnet/Gateway/DNS information for each appliance purchased

4) The Customer is responsible for the physical installation of the purchased appliances
5) The Customer is responsible for all physical network cabling and providing power in accordance with appliance specifications. CyFlare is NOT responsible for any physical network cabling or additional environmental items at the Customer's location
6) Customer responsible for all network configurations as required by the vendor for each technical solution being installed. CyFlare will provide details for each platform during the onboarding.
7) When applicable, the Customer will manage the operating system software installation of the supplied Windows/Linux server agent(s)
8) When applicable, the Customer will only install supplied Windows/Linux server agent(s) on identified servers (Not end workstations)
9) When applicable, the Customer will only install the number of Windows/Linux server agents identified and mutually agreed upon in writing.
10) When applicable, the Customer will configure Syslog senders in accordance with the number of senders identified and mutually agreed upon in writing.
11) When applicable, the Customer will provide API authentication tokens as needed for various integrations.
12) When applicable, the Customer will list existing vendor exclusions or whitelisted items used within the current endpoint security solution.
13) When applicable, the Customer will provide identification of servers, workstations, and laptops within scope for Sentinel One deployment.
14) When applicable, the Customer will identify sensitive endpoints involved in deployment that are mission-critical to business workflows to ensure proper Sentinel One installations.
15) When applicable, the Customer will manage the software installation of supplied Sentinel One software agents and tokens.
16) When applicable, the Customer will ensure vulnerability scanning tool requirements identified and mutually agreed upon in writing are satisfied.
17) When applicable, the Customer will ensure target systems within the scope of work have the necessary connectivity from the vulnerability scanning tool to perform scans.
18) When applicable, the Customer will ensure that the agreed upon vulnerability scanning timeframe is communicated to the organization to limit potential issues to production workflow.
19) When applicable, the Customer will provide current email system configurations related to transport rules and other system integrations that alter normal mail flow.
20) Configuration related to all DNS changes to Customer domains is the Customer's responsibility. If 3rd party vendors are involved with the required changes, the Customer must coordinate. CyFlare is not responsible for interactions with entities other than the Customer.
21) The Customer will participate and respond to CyFlare security tickets within ten days. After ten days, tickets within the CyFlare ticketing platform will auto-close without approval.
22) The customer is responsible for updating and ensuring the accuracy of the Incident Response plan used for escalations within CyFlare ONE.

## Scope of Individual Services

CyFlare shall provide the following for each respective in-scope services

# CyFlare mXDR O365, Initiate and Complete

- Execute an end customer-specific Incident Response plan as created in the ONE platform for escalations
- Monitoring of Customer deployed tenants, sensors, connectors, and log senders
- MXDR O365 Only: Microsoft 365 and Azure AD / EntraID monitoring only included
- Review initial events received and work with the Customer to tune the solution using a Customer-supplied context
- Customers are expected to share tuning requests with CyFlare when an unwanted escalation is received by opening a new case
- CyFlare will share curated detections with customers within CyFlare ONE platform.
- The list is updated periodically by CyFlare and can be found in the 'information' button in the upper right-hand corner of the ONE platform.

1) Monitor, investigate, and provide cases to Customers per the subscribed Service Level Agreement (24/7/365 monitoring based on XDR default CyFlare aligned detections)

- NOTE: Custom rules or Customer-created alerts that do not have an MITRE ATT&CK Framework ID may be subject to professional service fees for developing IR playbooks for those custom rules
- mXDR per-user licensing assumes an ingest ceiling of 60 megabytes/day times the licensed user count.
- For example, if 10 XDR users are licensed, a maximum ingestion of 600 mb/day will be expected. CyFlare reserves the right to, with Customer's express knowledge, shape service or adjust license counts if the maximum threshold is consistently surpassed for three consecutive months.

2) Join end-customer calls as requested in support of XDR platform tenants
3) Create filtering/exclusion rules required within the XDR platform

- Implement correlation rules as needed and subject to limits stated within the CyFlare Service Level Agreement located at: https://www.cyflare.com/legal/.
- For mXDR Complete Only: Enable Network Traffic Analysis functionality with related security detections (when the network sensor is deployed)
- For mXDR Complete Only: Enable core CyFlare XDR Defined Automation use cases identified in Table 1 on the next page
- Review initial events received and work with the Customer to tune the XDR solution using Customer supplied context builder
- If applicable, review, evaluate, and accommodate five custom requests per month from the Customer for new content. New content includes new curated security detections, dashboards, reports, or changes outside the default out-of-box security solutions offerings & standard processes.
- **Note**: all requests are subject to CyFlare approval or denial based on the internal evaluation. Any new content request requiring over 5 hours of development & implementation time may be subject to a flat fee.

CyFlare Security Inc.
950 Union Road, Suite 103
West Seneca, NY 14224

**P:** +1 877-729-3527
**E:** sales@cyflare.com

**Table 1**

| Service | Use Cases | | Common CyFlare Response Actions | Typical Integrations |
|---|---|---|---|---|
| mXDR | **Use Case 1** | **Firewall Policy Update:** Integration to make routine changes, such as adding an IP address to a blacklist or querying the whitelist. | • Write blacklist<br>• Read the blacklist (to see if it already had been added)<br>• Update geo-blocking from CKB (potential) | Juniper Networks, Cisco, Check Point, paloalto Networks, Fortinet |
| | **Use Case 2** | **Automated Notification System:** Send critical security alerts directly to team's comm channels, enabling faster response times and direct access to our ticketing system for streamlined incident resolution. | • Critical Escalations to Slack/Teams/SMS/Etc.<br>• Curate Custom Notifications on Detections (Volume, Severity, Timeframe, Etc..)<br>• Be Informed Instantly when Automation Response Occurs | xmatters, slack, Microsoft Teams |
| | **Use Case 3** | **Disable/Enable User Account**: This response action is invoked when there is a high probability the account or device has been compromised. To safeguard against account takeover and additional compromise, a user account can be disabled until properly investigated | • Enable User Account<br>• Lock User Account (permanently or for X amount of time) | okta, Google Cloud IAM, Active Directory, G Suite, CyberArk |
| | **Use Case 4** | **Email Integration:** Integrate to recall confirmed or potential phishing emails from mailboxes to minimize the risk of interacting with malicious URLs | • Quarantine email from mailbox(es) | mimecast, Office 365, Symantec, Harmony Email & Collaboration |

## CyFlare mXDR Connect

1) Support the SIEMs defined in ***Table 2 (see next page)*** for monitoring and response actions via API Integration

CyFlare Security Inc.
950 Union Road, Suite 103
West Seneca, NY 14224

**P:** +1 877-729-3527
**E:** sales@cyflare.com

2) Schedule regular integration sessions as needed during the onboarding
3) Execute on end customer-specific Incident Response plan as created in the ONE platform by customer
4) Regular Monitoring of API Connector status
5) Review initial events received and work with the Customer to tune the solution using a Customer-supplied context
    a) Customers are expected to share tuning requests with CyFlare when an unwanted escalation is received by opening a new case
6) Monitor, investigate, and provide cases to customers per the subscribed Service Level Agreement (24/7/365 monitoring).
    a) NOTE: Custom rules or Customer-created alerts that do not have an MITRE ATT&CK Framework ID may be subject to professional service fees for developing IR playbooks for those custom rules.
7) Join end-customer calls as requested.
8) Consult only on creating filtering/exclusion rules required within the SIEM platform
9) Consult only on implementing correlation rules as needed
10) If leveraging a Customer-provided SIEM solution, CyFlare will process all detections that are tagged with a MITRE ID.
    a) Detections sourced without a MITRE ID will be processed and visualized within the CyFlare ONE Platform.

**Table 2**

| SIEM Vendor | Response Actions Available | Ingest Detections |
|---|---|---|
| Stellar Cyber | Yes | Yes |
| AlienVault | Yes | Yes |
| Rapid7 InsightIDR | Yes | Yes |
| Arcsight | Yes | Yes |
| Devo | Yes | Yes |
| Elastic | Yes | Yes |
| FireEye Helix | Yes | Yes |
| Fortinet FortiSIEM | Yes | Yes |
| Google Chronicle | Yes | Yes |
| LogPoint | Yes | Yes |
| LogRhythm | Yes | Yes |
| Logzio | Yes | Yes |
| McAfeeESM | Yes | Yes |
| Microsoft Azure Sentinel | Yes | Yes |
| QRadar | Yes | Yes |
| RSA NetWitness | Yes | Yes |
| Splunk | Yes | Yes |
| Sumologic | Yes | Yes |
| Symantec ICDX | Yes | Yes |
| Vectra | Yes | Yes |

| | | |
|---|---|---|
| Humio | Yes | Yes |
| Nozomo Networks | Yes | Yes |

**Table 3**

| Feature / Benefit | mXDR Connect | mXDR O365 | mXDR Initiate | mXDR Complete |
|---|---|---|---|---|
| Onboarding / Deployment Assistance | ✓ | ✓ | ✓ | ✓ |
| Unlimited IR Support by SOC | ✓ | ✓ | ✓ | ✓ |
| 24x7 SOC Monitoring | ✓ | ✓ | ✓ | ✓ |
| XDR / SIEM Platform | BYO | ✓ | ✓ | ✓ |
| Advanced SLA | ✓ | ✓ | ✓ | ✓ |
| CyFlare ONE Platform | ✓ | ✓ | ✓ | ✓ |
| 97% True Positive Rate Target | ✓ | ✓ | ✓ | ✓ |
| UEBA, Machine Learning Detection Engines | BYO | ✓ | ✓ | ✓ |
| Threat Containment & Response Automation | ✓ | - | - | ✓ |
| Log Storage Retention | - | 90 Day Standard Optional 12 months Extended Log Retention | 90 Day Standard Optional 12 months Extended Log Retention | 90 Day Standard Optional 12 months Extended Log Retention |
| Network Traffic Analysis / Network Detection & Response | - | - | - | ✓ |

## CyFlare mEDR Connect & Complete

1) Execute on end customer-specific Incident Response plan as created in the ONE platform by customer
2) Review initial events received and work with the Customer to tune the solution using a Customer-supplied context

CyFlare Security Inc.
950 Union Road, Suite 103
West Seneca, NY 14224

**P:** +1 877-729-3527
**E:** sales@cyflare.com

- Customers are expected to share tuning requests with CyFlare when an unwanted escalation is received by opening a new case

3) Monitor, investigate, and provide cases to Customer per the subscribed Service Level Agreement (24/7/365 monitoring)
4) Join Customer calls as requested in support of end customers
5) Assist with Incident Response investigations that may require log searching and review to identify related events
6) mEDR Complete Only: Provide licensing for CrowdStrike, SentinelOne or Sophos EDR agents
7) mEDR Complete Only: Regularly manage/update agent versions as they become available
8) Enable core CyFlare mEDR Defined Automation use cases identified in Table 4 below

**Table 4**

| Service | Use Cases | | Common CyFlare Response Actions | Typical Integrations |
|---|---|---|---|---|
| mEDR | **Use Case 5** | **Scan/Remediate/ Rollback Endpoint:** Step two after isolation. Scan action will be part of the next steps after isolating the endpoint. Remediate and rollback will be done after contacting the customer and confirming the threat. | • Initiate AV scan<br>• Remediate (clean) threats<br>• Rollback machine | Carbon Black.<br>SOPHOS<br>SentinelOne<br>Symantec<br>CROWDSTRIKE |
| | **Use Case 6** | **Isolate/Unisolate Endpoint:** EDR integration to take response action on the endpoint in the event of a confirmed or likely threat. | • Shut down the machine<br>• Isolate from network<br>• Connect to the network | Carbon Black.<br>SOPHOS<br>CROWDSTRIKE<br>SentinelOne<br>Symantec |

**Table 5**

| Feature / Benefit | mEDR Connect | mEDR Complete |
|---|---|---|
| Onboarding and Deployment Assistance | ✓ | ✓ |
| Advanced SLA | ✓ | ✓ |

CyFlare Security Inc.
950 Union Road, Suite 103
West Seneca, NY 14224

**P:** +1 877-729-3527
**E:** sales@cyflare.com

| | | |
|---|---|---|
| Unlimited Incident Response | ✓ | ✓ |
| EDR Platform | BYO | ✓ |
| 24x7 SOC Monitoring | ✓ | ✓ |
| Automatic Threat Response & Containment | ✓ | ✓ |
| CyFlare ONE Platform | ✓ | ✓ |
| 97% True Positive Rate Target | ✓ | ✓ |
| Managed Agent Updates | - | ✓ |
| Policy Creation & Management | - | ✓ |

**Table 6**

| EDR / AEP Platform Vendor | Response Actions Available | Ingest Detections |
|---|---|---|
| SentinelOne | Yes | Yes |
| Sophos | Yes | Yes |
| Crowdstrike Falcon | Yes | Yes |
| Bitdefender Gravity Zone | Yes | No |
| VmWare Carbon Black Cloud | Yes | Yes |
| VMWare Carbon Black Enterprise EDR | Yes | No |
| VMWare Carbon Black Endpoint Standard | Yes | No |
| Carbon Black Defense | Yes | No |
| Carbon Black Response | Yes | Yes |
| Carbon Black Protection | Yes | No |
| Cisco AMP | Yes | Yes |
| Cybereason | Yes | Yes |
| Cylance | Yes | Yes |
| Cynet | Yes | No |
| Endgame | Yes | Yes |
| Extrahop | No | Yes |
| FireEye HX | Yes | Yes |
| Google Rapid Response | Yes | No |
| Ivanti | Yes | No |
| McAfee Active Response | Yes | No |
| McAfee EPO | Yes | Yes |

CyFlare Security Inc.
950 Union Road, Suite 103
West Seneca, NY 14224

**P:** +1 877-729-3527
**E:** sales@cyflare.com

| | | |
|---|---|---|
| McAfee Mvision EDR | Yes | Yes |
| McAfee Mvision EPO | Yes | Yes |
| Microsoft 365 Defender | Yes | Yes |
| Microsoft Defender ATP | Yes | Yes |
| Microsoft Intune | Yes | No |
| Observe IT | No | Yes |
| Orca Security | Yes | Yes |
| Palo Alto Cortex XDR | Yes | Yes |
| Qualys EDR | No | Yes |
| RSA Witness EDR | Yes | No |
| Symantec Endpoint Protection | Yes | No |
| Trend Micro Security | Yes | No |
| Armis | Yes | Yes |
| Azure Security Center | Yes | Yes |
| OpSWAT | Yes | No |
| ProofPoint TAP | Yes | No |
| Tanium | Yes | No |

# CyFlare Vulnerability Scanning Services (VSS) Lite & Enhanced

*Previously Cyber Risk Intelligence (CRI)*

1) Provide vulnerability scanning solution including recommended scan templates and guidance
2) Assist in vulnerability scanning design and architecture creation
   a) Identify external scanning targets
   b) Identify in-scope network scan subnets
   c) Identify machines requiring deployed scanning agent
   d) Configure Customer-requested scan schedules
   e) Configure Customer-provided credentials where required to enable authenticated scans
3) Provide agent licensing
4) Configure automated reporting to email target
5) VSS Lite Only: Alert Customer Incident Handler when dark web hits occur
6) Configure Azure AD integration using Customer-provided API credentials
7) Continuous monitoring of operational health checks that include:
   a) Scan job completion
   b) Expired credentials
8) Regularly update agents as they become generally available
9) If applicable, provide a vulnerability scanning report generated by the scanning platform via email

10) If applicable, the configuration of the vulnerability scanning tool in accordance with recommended best practices of the platform (provide installation agent to Customer if applicable)

**Table 7**

| Feature / Benefit | VSS Lite | VSS Enhanced |
|---|---|---|
| Vulnerability Scanning Strategy Development | ✓ | ✓ |
| Scanning Architecture Development | ✓ | ✓ |
| Configure Scanning Jobs | ✓ | ✓ |
| Continuous Health Checks | ✓ | ✓ |
| Internal/External Vulnerability Scanning | ✓ | ✓ |
| Dark Web Monitoring & Alerting | ✓ | |
| Active Directory Insights | ✓ | |
| Ongoing Configuration Management | ✓ | ✓ |
| Operational Dashboard (Coverage) | ✓ | ✓ |
| Patching w/Virtual Patch Technology | | ✓ |
| CyFlare mXDR Integration (Insights) | | ✓ |

## CyFlare Managed Email Security (mES)

1) Provide email security solution and licensing
2) Integrate email security tenant with customer environment leveraging API
3) Provide customer access to email security platform
4) Configure email security settings and controls within platform using vendor best practices
5) Integrate mES services with CyFlare SOC for alerting and investigations
6) Configure email security reporting analytics as requested by customer

**Table 8**

| Feature / Benefit | mES Basic | mES Advanced | mES Complete |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Secure All Email (Inbound, Outbound, Internal) | ✓ | ✓ | ✓ |
| Advanced AI-Based Anti-Phishing | ✓ | ✓ | ✓ |
| Anti-Spam Filtering | ✓ | ✓ | ✓ |
| Known Malware Prevention | ✓ | ✓ | ✓ |
| Protection from Zero-Day Malware (File Sandboxing) | | ✓ | ✓ |
| File Sanitization (CDR) | | ✓ | ✓ |
| Malicious URL Protection | ✓ | ✓ | ✓ |
| URL Click-time Protection | ✓ | ✓ | ✓ |
| Zero-Day Malicious URL Protection | | ✓ | ✓ |
| Account Takeover Protection | ✓ | ✓ | ✓ |
| Unauthorized App Detection | ✓ | ✓ | ✓ |
| Data Loss Prevention | | | ✓ |
| Encryption | | | ✓ |

CyFlare Security Inc.
950 Union Road, Suite 103
West Seneca, NY 14224

**P:** +1 877-729-3527
**E:** sales@cyflare.com